

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 64-004139

(43)Date of publication of application : 09.01.1989

(51)Int.Cl.

H04L 9/00
G09C 1/00

(21)Application number : 62-157602

(71)Applicant : NEC CORP

(22)Date of filing : 26.06.1987

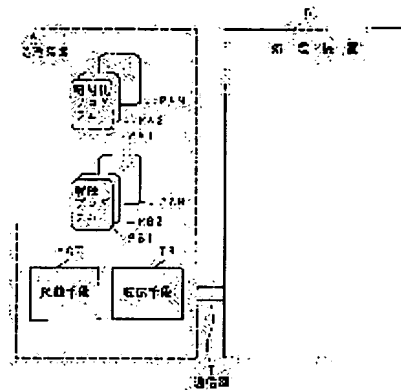
(72)Inventor : IDEMURA SHIGEO

(54) ENCIPHERMENT SYSTEM

(57)Abstract:

PURPOSE: To prevent the interception of a decoded program and a transfer data by allowing a master equipment to select one of various kinds of decoding programs and transferring it to an opposite slave equipment prior to data transmission.

CONSTITUTION: A processor A is provided with data encipherment programs PA1 ~ PAN operated on the processor. A and cipher decoding programs PB 1 ~ PBN operated on a processor B. Then the processor A determines a cipher to be implemented, selects one of encipherment programs PA1, PA2 ~ PAN operated on the processor A, selects a decoding program among the programs PB1, PB2...PBN operated on the processor B, transfers it by a transmission means TR to execute the encipherment data transfer thereafter.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

BEST AVAILABLE COPY

Copyright (C); 1998,2003 Japan Patent Office

⑩ 日本国特許庁(JP)

⑪ 特許出願公開

⑫ 公開特許公報(A)

昭64-4139

⑬ Int.Cl.

識別記号

庁内整理番号

⑭ 公開 昭和64年(1989)1月9日

H 04 L 9/00
G 09 C 1/00Z-7240-5K
7368-5B

審査請求 未請求 発明の数 1 (全4頁)

⑮ 発明の名称 暗号化方式

⑯ 特 願 昭62-157602

⑰ 出 願 昭62(1987)6月26日

⑱ 発 明 者 井 出 村 重 夫 東京都港区芝5丁目33番1号 日本電気株式会社内
 ⑲ 出 願 人 日本電気株式会社 東京都港区芝5丁目33番1号
 ⑳ 代 理 人 弁理士 井出 直孝

明 細 書

1. 発明の名称

暗号化方式

2. 特許請求の範囲

(1) 主装置および主装置と通信網を介して接続された従装置との間でこの通信網を介して行うデータ通信の暗号化方式において、

暗号データの送信に先立って、上記主装置から上記従装置に対して暗号解読の論理を含む解読プログラムを伝送し、

この解読プログラムを受信した従装置は、この解読プログラムをメモリに格納し、

上記主装置は、上記従装置を制御して上記メモリに格納された解読プログラムを起動させ、

その後暗号通信を実行する

ことを特徴とする暗号化方式。

3. 発明の詳細な説明

〔産業上の利用分野〕

本発明は、データ通信の暗号化方式に関する。特に、通信路の両終端が独自の処理能力を有する装置間のデータ通信の暗号化に関するものである。

〔概 要〕

本発明はデータ通信の暗号化方式において、

主装置は多数種の解読プログラムを持ち、そのうちの一つを選択して相手従局に転送し、相手従局は転送された解読プログラムを受信し格納し、また主局はこの解読プログラムを起動して暗号データを転送し、相手従局はこの解読プログラムで解読を行うことにより、

解読プログラムの盗用および転送データの盗用を防止し、また解読プログラムが盗まれた際の系全体での暗号の変更を容易にすることができ、かつ開かれた通信路上で規格外の処理装置のアクセスを防止できるようにしたものである。

〔従来の技術〕

従来データ通信の暗号化方式は、暗号に関する

手段は通信を行う処理装置が各自の装置上で動作するものを保持しており、データの転送に先立ってその転送に関する暗号の記法を選択するデータの転送を行い記法を決定するか、または固定的に一意な記法を決定するかして暗号化を行っていた。

〔発明が解決しようとする問題点〕

しかし、このような従来のデータ通信の暗号化方式では、暗号に関する手段が通信を行う処理装置の上に固定的に存在しているために、解読プログラムの盗用および短時間の暗号データを頻繁に通信路から盗み出すことによる暗号化記法の推察によってデータが盗まれ解読されることを防止することが困難で、また、暗号化記法が盗まれていることが判明した場合でも、特に、同一の暗号化記法を用いる装置が多数存在する系では、暗号に関する手段を一時期に置換しなければならず、実際の問題としてこのことが非常に困難である欠点があった。

本発明は上記の欠点を解決するもので、解読プログラムの盗用および転送データの盗用を防止で

き、かつ開かれた通信路上で規格外の処理装置のアクセスを防止できる暗号化方式を提供することを目的とする。

〔問題点を解決するための手段〕

本発明は、主装置および主装置と通信網を介して接続された従装置との間でこの通信網を介して行うデータ通信の暗号化方式において、暗号データの送信に先立って、上記主装置から上記従装置に対して暗号解読の論理を含む解読プログラムを送信し、この解読プログラムを受信した従装置は、この解読プログラムをメモリに格納し、上記主装置は、上記従装置を制御して上記メモリに格納された解読プログラムを起動させ、その後暗号通信を実行することを特徴とする。

〔作 用〕

主装置は、多数種の解読プログラムのうちの一つを選択してデータ転送に先立ってこれを相手の従装置に転送する。さらにこの解読プログラムを起動する。相手の従装置は転送されてくるあるいは転送するデータをこの解読プログラムで解読ま

たは暗号化する。一連の通信の終了後にこの解読プログラムは消去してもよい。

これにより、従装置では次に伝送される暗号の解読プログラムを蓄えておかないので、解読プログラムの盗用の可能性が少なくなる。また解読プログラムの種類はきわめて多くすることができ、たとえ解読プログラムを盗用しても、それが利用できる可能性はきわめて小さくなる。

ひんばんに短時間のデータ転送を行う系で、その度に解読プログラムを転送することが実用的でない場合には、従装置では転送されてきた解読プログラムを通信の終了後も保持し再利用することもできる。この場合でも主処理装置は欲する時点で通信の開始前に解読プログラムを置換することが可能であり本発明の利点を大きく損なわない。

たとえば、各従局にキーワードを設定しておき、各従局は主局への応答またはアクセスを行うときには、このキーワードを受信格納した解読プログラムにしたがって暗号化して伝送するようにしておけば、かりに通信回線を傍受してキーワードパ

ターンを盗んでも、そのキーワードパターンは暗号化されたものであり、次の通信では別の暗号論理になっているから利用できない。

全体の通信時間のうち解読プログラムを転送する時間は一般にきわめて短いので、解読プログラムが盗まれる可能性は小さい。

〔実施例〕

本発明の実施例について図面を参照して説明する。

第1図は本発明の第一実施例暗号化装置のブロック構成図である。第1図において、暗号化装置は、処理装置Aと、処理装置Aに通信路Tを介して接続された処理装置Bとを備える。処理装置Aは、処理装置A上で動作するデータの暗号化プログラムPA1～PANと、この暗号化プログラムPA1～PANにそれぞれ対応して処理装置B上で動作する暗号の解読プログラムPB1～PBNと、選択した暗号化プログラムPAに対応する解読プログラムPBを処理装置Bへ転送する転送手段TRと、転送した解読プログラムPBを起動す

る起動手段ACTを含む。

このような構成の暗号化装置の動作について説明する。第1図において、本発明の第一実施例は、一連のデータ転送に先立って必ずプログラムを転送する場合である。

第2図は本発明の第二実施例暗号化装置のブロック構成図である。第2図において、処理装置Aはこれから行う暗号の決定を行い、処理装置A上で動作する暗号化プログラムPA1、PA2、……、PANの中から一つを選択する。そしてこれに対応する処理装置B上で動作する解読プログラムをPB1、PB2、……、PBNの中から選択し、これを転送手段TRによって転送し、さらに、起動手段ACTによって起動を行った後に、暗号化データ転送を実行する。

この第二実施例は、転送を行おうとする解読プログラムがすでに相手処理装置上に存在する場合に、転送を行わずすでに存在する解読プログラムを起動する場合である。第一実施例において処理装置Bは転送されてきた処理装置B上で動作する

解読プログラムを記憶しているとする、何度かのデータ転送の後には第2図に示すような状態となる。ここで処理装置Aはデータ転送を行う際には、暗号の決定を行いそれに対応する処理装置B上で動作する解読プログラムを選択し、まず起動手段ACTによってこの解読プログラムの起動を行う。選択したプログラムが解読プログラムPB1であった場合には、解読プログラムPB1が処理装置B上に存在しないのでエラーが通知され、この場合には第一実施例と同様の動作を行う。選択したプログラムが解読プログラムPB2であった場合には、解読プログラムPB2が処理装置B上に存在するので起動は成功する。ここで起動した解読プログラムPB2が欲しているプログラムであるかどうかのチェックが行われ、欲しているプログラムでなければ起動した解読プログラムPB2を終了させ第一実施例と同様の動作を行う。欲しているプログラムであればそれを用いて暗号化データ転送を行う。

第3図は本発明の暗号化装置が適用される開か

れたデータ通信装置のブロック構成図である。処理装置AをホストコンピュータCP、処理装置BをワークステーションWSおよび各暗号化プログラムを各々のシステム上の暗号化プログラムとして第3図に示すように公衆通信網Nを介してホストコンピュータCPとワークステーションWS1、……、WSNとが通信を行う際にアクセス権のチェックを本発明に従って行う場合を考える。公衆通信網Nを介して転送されてくる解読プログラムを動作させ得るワークステーションWS1、……、WSNを使用してアクセス権を示すキーワードを知っている利用者は問題なくホストコンピュータCPへアクセスできるが、転送されてくる解読プログラムを動作させ得ない端局装置TMを使用してアクセスを行おうとする利用者および通信網上を流れる暗号化されたキーワードのイメージのみを知っている利用者がホストコンピュータCPにアクセスすることはできなくなっている。

〔発明の効果〕

以上説明したように、本発明は、通信路上の全

データが所定時間以上連続して盗み見られないような環境下で、系内のアクセス権チェック用データ等の比較的短い重要なデータの盗用を防止することを可能とし、また公衆通信網等の開かれた通信路上から規格外の処理装置で系内にアクセスしてくることを防止できる優れた効果がある。

4. 図面の簡単な説明

第1図は本発明の第一実施例暗号化装置のブロック構成図。

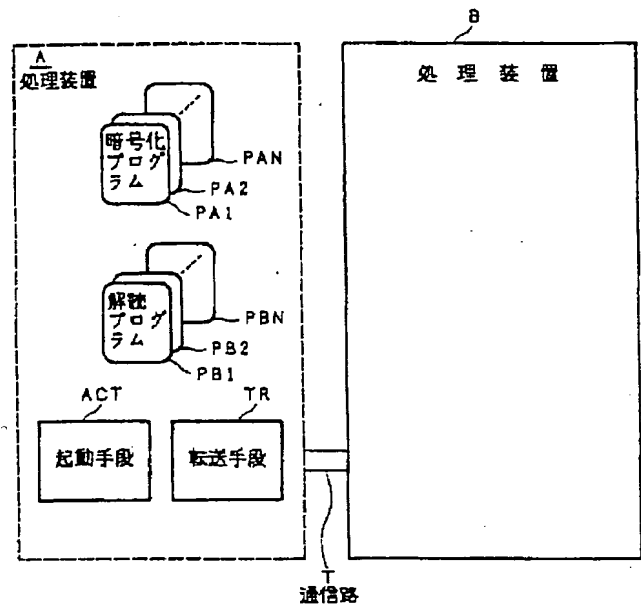
第2図は本発明の第二実施例暗号化装置のブロック構成図。

第3図は本発明の暗号化装置が適用される開かれたデータ通信装置のブロック構成図。

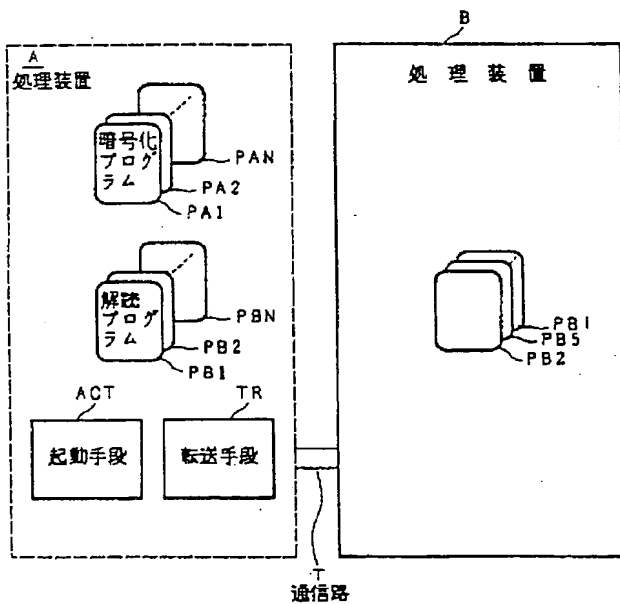
A、B…処理装置、ACT…起動手段、CP…ホストコンピュータ、N…公衆通信網、PA1～PAN…暗号化プログラム、PB1～PBN…解読プログラム、T…通信路、TM…解読プログラムを動作させ得ない規格外端局装置、TR…転送手段、WS1～WSN…解読プログラムを動作さ

せ得るワークステーション。

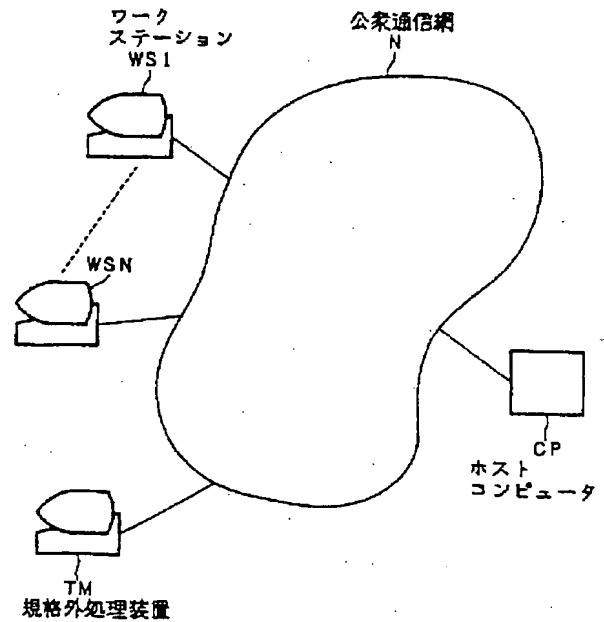
特許出願人 日本電気株式会社
代理人 弁理士 井出直孝



第一実施例
第 1 図



第二実施例
第 2 図



実施例データ通信装置
第 3 図